UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,390	01/22/2001	Kazue Sako	043034/0164	1020

22428 7590 10/20/2005

FOLEY AND LARDNER LLP
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
DADA, BEEMNET W	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 10/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/765,390	SAKO, KAZUE	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9,12,15 and 18-22* is/are rejected.

7)☒ Claim(s) *7,8,10,11,13,14,16 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The request filed on July 27, 2005 for a request for Continued Examination (RCE) under 37 CFR 1.114 based on parent Application 09/765,390 is acceptable and an RCE has been established. Claims 1, 10 and 18 have been amended. Claims 1-22 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 9, 12, 15 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ateniese et al. "Some Open Issues and New Directions in Group Signatures" (hereinafter Ateniese) in view of Jakobsson US Patent No. 6,317,833 B1.

4. As per claims 1 and 18, Ateniese discloses a participant subsystem (see for exsample: signer page 207 section 10) that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem (see for example, group manager, page 197 section 2); and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session (see for example, verify page 207, section 10),

wherein the participant subsystem comprises:

an anonymous signing section for authorizing individual data using the secret information depending on session-related information (see for example, one time base g, page

207 section 10) to produce anonymous participation data with anonymous signature, and the reception subsystem comprises (see for example, group signature, page 207, section 10);

an anonymous signature determining section for determining whether received data is anonymous participation data (see for example, verify, page 207, section 10) with anonymous signature authorized by the participant subsystem; and a sender match determining section for determining whether anonymous signatures of arbitrary two pieces ($V_{1,i}$, $V_{2,j}$) of anonymous participation data are signed by an identical participant subsystem (see for example, same g must be used, page 207 section 10). Ateniese is silent on secret information being transmitted to participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of session. However, within the same field of endeavor Jakobsson teaches an anonymous participation system, including secret information being transmitted to participant subsystem prior to participation in a first of said plurality of sessions, said secret information enabling participation in each of the plurality of session [see column 2, lines 40-63]. Both Ateniese and Jakobsson teach an anonymous participation system. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Jakobsson within the method of Ateniese in order to provide participant subsystems with necessary information to participate in current and/or future session.

5. As per claims 2 and 19, Ateniese further teaches the method wherein the anonymous signature includes data that is generated by a predetermined expression (see for example, group signature page 205 paragraph 2 and page 207 section 10) using the session-related Information and the secret information, wherein the sender match determining section checks

the data included in the anonymous signature of received anonymous participation data (see for example, page 207, section 10 paragraph 5).

6. As per claims 3 and 20, Ateniese discloses the method wherein the predetermined expression is represented by raising a session-dependent base (g) to a power that is dependent on the secret information (see for example, page 204, paragraphs 3-4 and page 207, section 10).

7. As per claims 4, Ateniese discloses the method wherein the anonymous signing section authorizes the individual data based on a group signature scheme (see for example, page 198-199, section 3).

8. As per claim 5, Ateniese discloses the method wherein the anonymous signing section authorizes the individual data based on an escrowed identity scheme (see for example, OPEN page 197).

9. As per claim 6 and 21, Ateniese discloses the method wherein the anonymous signing section comprises: a generator creating section for creating a session-dependent generator depending on the session-related information (see for example, trusted entity to generate, page 210, section 10.3); a group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data (see for example, group signature over a message, page 104, and one-time base page 207 section 10), wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information (see for

example, V_1:=..., page 204); and a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information (see for example, page 207, section 10 paragraph 5).

10. As per claims 9 and 22, similar limitations are described in claims 6 and 21 above and are rejected under the same rationale.

11. As per claim 12, Ateniese discloses the method wherein the anonymous signing section comprises: a generator creating section for creating a session-dependent generator depending on the session-related information (see for example, trusted entity to generate, page 210, section 10.3); an escrow identifying section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data (see for example group signature over a message page 104 and one-time base page 207 section 10) , wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information (see for example, V_1:=..., page 204); and a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the individual data and/or the session-related information (see for example page 207, section 10 paragraph 5).

12. As per claim 15, Similar limitations are recited in claim 13 above and are rejected under the same rationale.

Allowable Subject Matter

13. Claims 7, 8, 10, 11, 13, 14, 16 and 17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

14. Applicant's arguments filed July 27, 2005 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

October 16, 2005

Primary Examiner
Art Unit 2135